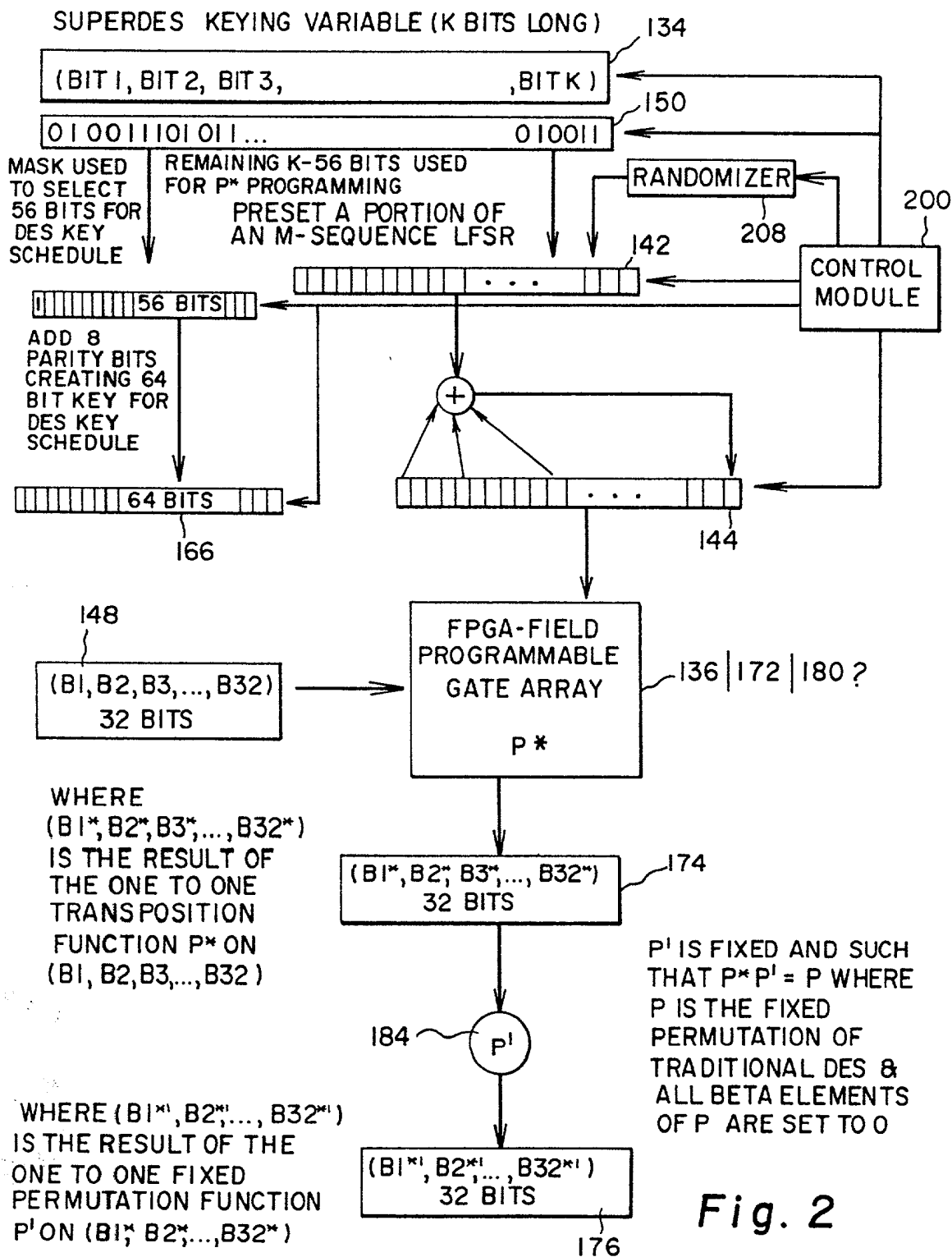


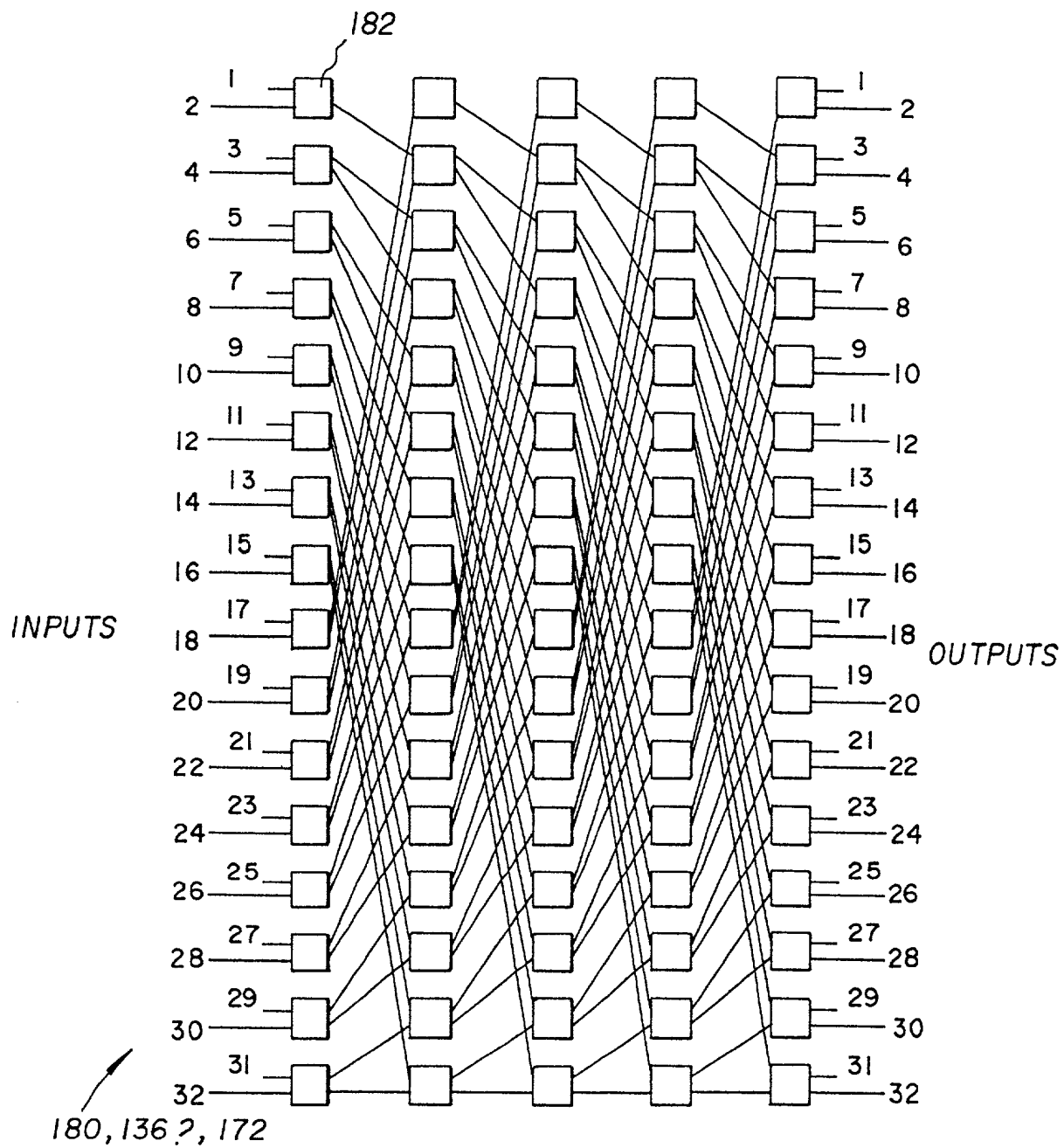
The diagram illustrates a cryptographic algorithm's structure. It begins with an **INPUT** block (64) labeled 110. This input passes through an **INITIAL PERMUTATION** block (112). The output of the initial permutation is split into two paths: **L0** (114) and **R0** (116). These paths enter a series of iterative rounds, with the first round explicitly showing a function **f** (120) applied to **R0** and a key **K1** (118) being added to the result (122). The output of this round is then split into **L1 = R0** and **R1 = L0 + f(R0, K1)**. This process repeats for subsequent rounds, with keys **K2**, **Kn**, and **Kn+1** being used. The final round shown is labeled 126, where the output is **PRE-OUTPUT** (126). The pre-output is then processed by an **INVERSE INITIAL PERM.** block (130) to produce the final **OUTPUT** (64) labeled 132. The entire iterative process is enclosed in a dashed box labeled 124.

108

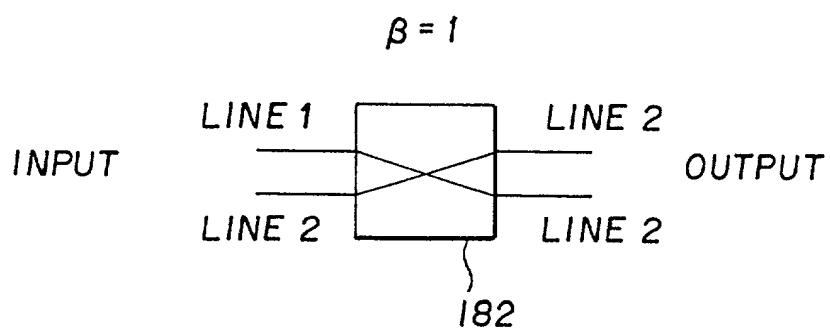
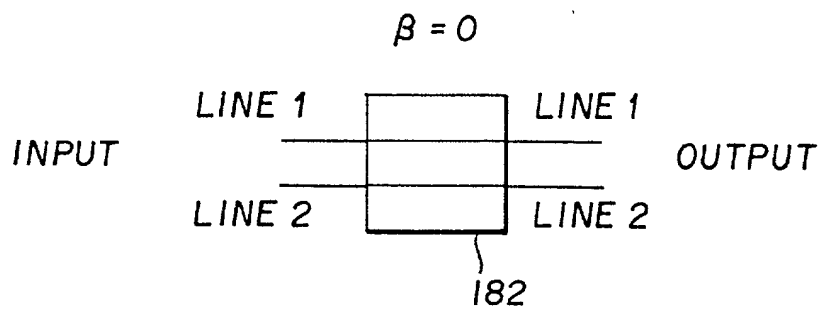


**Fig. 2**

120



**Fig. 4**



*Fig. 5*

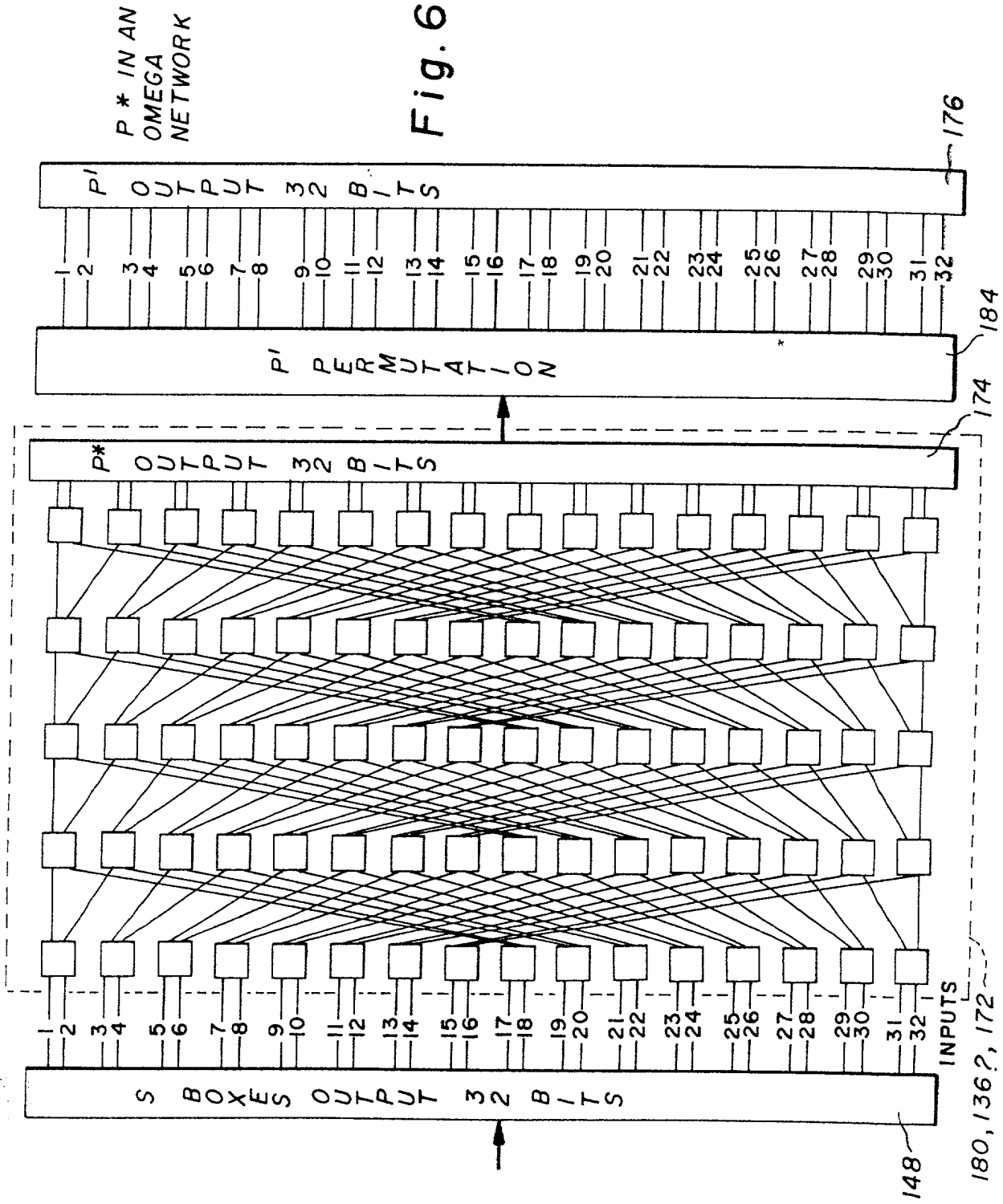


Fig. 6

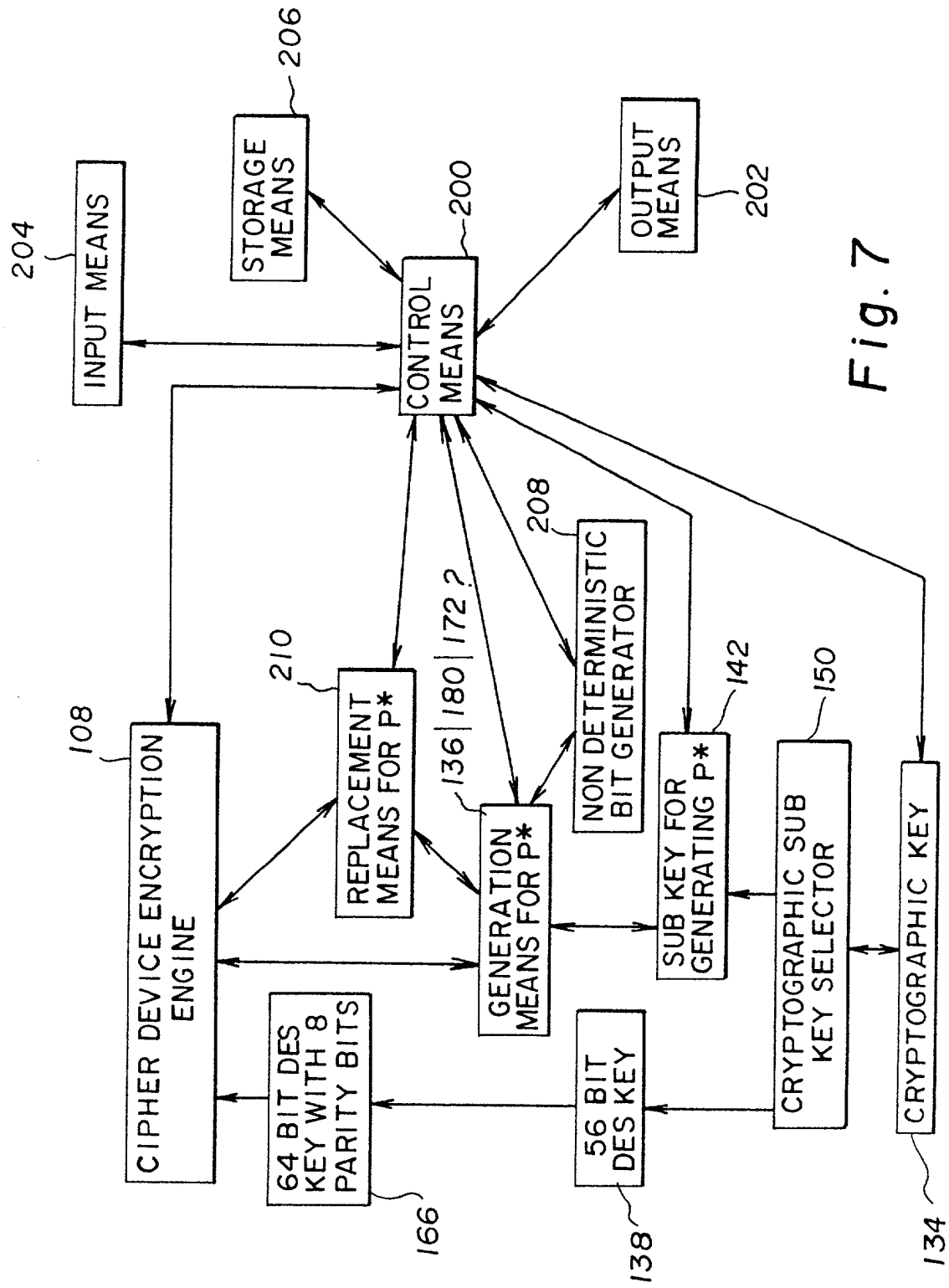


Fig. 7

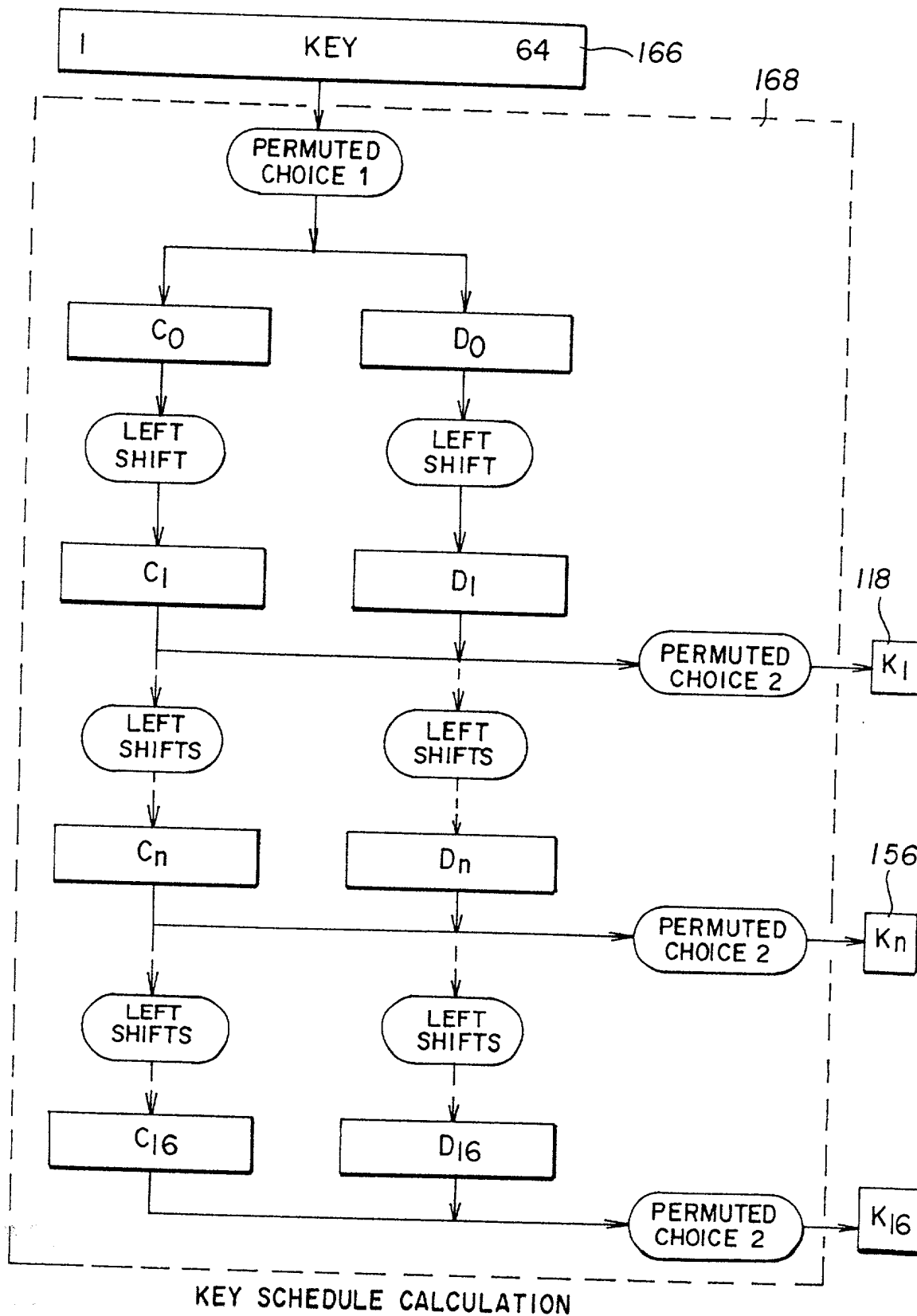


Fig. 8